LOS ANGELES TIMES
17 June 1985

Change in Soviets' Sub Tactics Tied to Spy Case

Material Reportedly Available to Walkers May Have Tipped Kremlin to Vessels' Vulnerability

By ROBERT C. TOTH, *Times Staff Writer*

WASHINGTON—As the Soviet Union's missile-carrying submarines emerge from their home waters, American attack submarines take up their trails and hover undetected close behind. So near do the U.S. hunter-killers get, often within 200 yards, that Navy officials believe that they could hear the hatches on a Soviet craft open and might be able to destroy it before its nuclear-tipped missiles could be launched.

After 20 years of emphasizing speed, however, the Soviets about 10 years ago began concentrating on making their submarines quieter and, thus, more difficult to detect and trail. And the big new Soviet Typhoon submarines with their longer-range missiles, instead of being sent out on distant patrols where they were vulnerable to American hunter-killers, now are being deployed in the more easily protected "water bastions" of the Arctic Ocean and the Sea of Okhotsk.

'Boomers' Vulnerable

Today, as they analyze the damage done by the "all in the family" spy ring allegedly headed by John A. Walker Jr., the former Navy chief warrant officer, intelligence officials suspect that it was because of information from Walker that the Soviets came to realize how vulnerable their missile subs (or "boomers," as such submarines are called) really were.

And the possibility that such information may have contributed to major changes in Moscow's nuclear submarine strategy suggests how deep the damage done by the Walker spy case may be.

Thus, despite the Navy's assurances last week that it largely has identified the damage, spillover from the sensational case continues to spread as Congress and other government agencies seek to discover the full scope of the espionage and its effects.

Pentagon officials indicated that they will be reluctant to accept the Navy's view that the outer limits of compromised secrets are known until the motives of Walker and the other members of the alleged spy ring—his son, Michael Lance, 22, a sailor; his brother, Arthur J., 50, a retired lieutenant commander and employee of a defense contractor, and his friend, Jerry A. Whitworth, a retired Navy communications specialist—are more clearly understood.

"For sure, it wasn't communist ideology," one knowledgeable defense official said. "Walker seems to be to the right of Attila the Hun. Why did the son and brother join him? There's a limit to family loyalty. And they didn't get very much money out of it—less than $100,000 over almost two decades all together.

"(Defense Secretary Caspar W.) Weinberger keeps asking: 'Why did they do it?' The Walkers are not cooperating, so we still just don't know."

Until they do, the Defense Department and the entire national security establishment probably will not be satisfied that the damage is being contained. Knowing a spy's motives can provide valuable clues to otherwise unsuspected areas that he might have sought to penetrate.

Navy's Worst Scandal

The scandal is clearly the worst in U.S. Navy history, and, eventually, may rank among the worst in the nation's history. Rather than "a mile wide and an inch deep" as first suspected, "it's more like a block, just about as deep as it is wide," one expert said.

"There are continuing examinations going on to get at the full extent of the damage," Weinberger said in an interview. "It went on for 18 years, and there've been serious losses, no doubt about that."

Of the four men, John Walker and Whitworth had access to the most damaging material. This included encoding machines and associated keying material, communications to and from U.S. missile submarines and reports on the performance of anti-submarine warfare tactics by U.S. attack submarines against Soviet vessels, several experts in this field said.

The Navy's top officer, Adm. James D. Watkins, said anti-submarine warfare was the area of greatest potential damage from the alleged spy ring, which presumably gave the Soviets access to secret voice and Teletype messages.

Such messages, according to Adm. Bobby R. Inman, former deputy director of the Central Intelligence Agency, could "reveal details on how we went about detecting Soviet units, the effectiveness of it, our tactics in peacetime and what tactics we might use in crisis. . . . But the damage here could be long-lasting," he said in an interview, because the string of U.S. sonar and other listening systems embedded in ocean floors is supposed to remain in place for years.

Defending Against Subs

What may be one of the most serious and long-lasting effects of the case involves the U.S. ability to defend against Soviet nuclear missile submarines.

Navy attack submarines of the Los Angeles class pick up Soviet missile-carrying submarines as they emerge from the Norwegian Sea into the North Atlantic Ocean and from Vladivostok as they move into the North Pacific Ocean.

The Soviet vessels are trailed throughout their patrols.

Intelligence officials now suspect that, thanks to the alleged spy ring's information, the Soviets became aware of the extent of their missile subs' vulnerability. In addition to shifting its priorities to quieter operations and developing tactics for keeping its biggest undersea vessels in safer waters, Moscow also stepped up efforts aimed at detecting U.S. subs, these officials believe.

In contrast to the major 1975 worldwide Soviet naval maneuvers, called "Okean '75," when

CONTINUED

2

Soviet tactics emphasized projecting power into distant waters and cutting Western sea lanes, more recent maneuvers have focused on finding and destroying enemy submarines and protecting their own missile subs—changes that could have been influenced by the alleged Walker revelations.

As a result of the Soviet change of tactics, the role of the American hunter-killer submarines is growing more difficult and more dangerous. And, with the Soviets' giant Typhoon subs no longer making long open-sea patrols, an increasing part of Moscow's missile submarine fleet is less exposed to U.S. attackers.

Intelligence professionals believe the Kremlin may have reaped a second major windfall from the Walkers' access to cryptographic material and coded messages.

The Soviet Union, like the United States, records all electronic signals it picks up and files them all in library-like systems. Both nations also change their codes every day, but the files are kept in hope that past messages someday can be deciphered—offering valuable information about an opponent's tactics, command systems and other matters that would provide a significant advantage in a war.

The clear text of secret messages allegedly passed to them by Walker could be used by the Soviets in this way. Using information about the frequency and other details of the U.S. transmissions, and retrieving coded messages recorded previously, then comparing the clear text with the coded text, the Soviets could break the code for all messages sent on that day.

Military Communications

Communications on that day between the Navy and other U.S. and allied military services, as well as with other U.S. agencies, also would be decipherable once the code was broken.

The Soviets could extract additional information from breaking even one day's code. Knowledge of how the code was constructed, plus data on U.S. cryptographic machines also allegedly provided by the ring, would have given Moscow's code-breakers better chances of cracking U.S. codes used on other days, intelligence sources said.

The code machines in the most sensitive U.S. communications centers (such as the White House Situation Room) are changed regularly, both as precautionary measures and as improved machines and encoding systems become available. But for communication at a tactical level, such as in submarines and at fleet and division headquarters, each service and agency decides if and when to buy new equipment.

The services, including the Navy and Army, often defer new purchases of expensive coding apparatus unless there is evidence that the existing machines have been compromised. The Navy may well have been slow in replacing its older machines, purely for financial reasons. This could explain why it now faces expenditures of "many millions of dollars," as Navy Secretary John F. Lehman Jr. estimated, to buy substitutes for the now-compromised equipment.

At least one more complicating factor is that older coding equipment in service must be able to communicate with newer equipment, and vice versa. This has raised the possibility—highly improbable, experts said, but not impossible—that encryption equipment more sophisticated than the 15-year-old machines available to the Walkers may also have been compromised.

Ripples of apprehension resulted from all these questions last week, including:

—The Army, Marines and Air Force created task forces to study the impact of the Walker case on each service, and the National Security Agency, which makes code machines and encryption systems for all of the government, set up "study groups" to examine repercussions on its activities.

—The Senate Intelligence Committee embarked on a "comprehensive review" of Soviet intelligence activities and U.S. counterintelligence efforts, which will include examination of the broad national security implications of the Walker case. The House Intelligence Committee, after a detailed briefing on the case, focused on remedial steps that have been proposed, including random polygraph lie detector tests.

Meanwhile, intelligence professionals are withholding judgment on how badly U.S. national security has been damaged. Where the Walkers eventually will rank on the scale of sensational espionage cases also still is in doubt.

The theft of atomic weapons secrets during World War II by the Fuchs-Rosenberg ring clearly was the worst espionage loss this country has experienced. The sale of information about U.S. spy satellites in the 1970s in two celebrated cases—involving "the Falcon and the Snowman," Christopher Boyce and Daulton Lee at TRW Corp., and William Kampiles at the CIA—severely cut the value of U.S. reconnaissance spacecraft, but the damage was limited to a single subject and repaired when new satellites were designed and launched.

But at least two members of the alleged spy ring, John Walker and Whitworth, had access to secret information across a broader range of subjects. Their alleged crimes are more comparable, in the view of two sources, to the treason of Army Sgt. Jack E. Dunlap.

A courier between sections of the NSA, Dunlap stole many of the nation's most highly secret messages for the Soviets from 1960 to 1963, when he committed suicide rather than face trial.

After Dunlap was caught, the NSA in the mid-1960s undertook thorough reform of its security procedures, including briefcase searches and polygraph tests. The CIA, after Kampiles' sale of a technical manual on the super-secret satellite, instituted the same procedures.

In the wake of the Walker case, the Navy says, it now plans to adopt similar changes to protect its secrets.